United States Department of Justice
Office of the Inspector General
Audit Division

Audit Report

Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2002

The United States Marshals Service's Warrant Information Network

November 2002

03-03

INDEPENDENT EVALUATION PURSUANT TO THE GOVERNMENT INFORMATION SECURITY REFORM ACT FISCAL YEAR 2002

THE UNITED STATES MARSHALS SERVICE'S WARRANT INFORMATION NETWORK

OFFICE OF THE INSPECTOR GENERAL EXECUTIVE SUMMARY

The mission of the United States Marshals Service (USMS) is to protect the Federal courts and ensure the effective operation of the judicial system. Specifically, the USMS is responsible for providing protection for the federal judiciary, transporting federal prisoners, protecting endangered federal witnesses, and managing assets seized from criminal enterprises.

The Warrant Information Network (WIN) contains the warrant, court records, internal correspondence related to the warrant, and other information on individuals for whom federal warrants have been issued. WIN is used to track the status of all federal warrants to aid in the investigations of all federal fugitives. It is also used to access the National Law Enforcement Telecommunication System (NLETS) and National Crime Information Center (NCIC) systems to obtain criminal record information from other federal, state, local and foreign law enforcement agencies participating in or cooperating with USMS fugitive investigations and apprehension efforts and to update the respective systems with new prisoner information.

WIN is accessed by both USMS district offices and headquarters users through the Marshal Network (MNET). MNET is the backbone unclassified network for USMS operations. MNET is a sensitive but unclassified system that provides office automation tools to USMS personnel in carrying out their worldwide mission. MNET is accessible from field sites and from certain other federal agencies and commercial organizations.

The Office of the Inspector General (OIG) was required by the Government Information Security Reform Act (GISRA) to perform an independent evaluation of the United States Department of Justice (Department) information security program and practices. The OIG selected WIN as one of five sensitive but unclassified systems to review pursuant to GISRA for the fiscal year 2002. However, because of WIN's dependence on MNET, audit work was expanded to include MNET as well.

Under the direction of the OIG and in accordance with Government Auditing Standards, PricewaterhouseCoopers LLP (PwC) performed the audits of WIN and MNET. This report contains the audit results of the WIN and MNET systems. Separate reports will be issued for each of the other systems evaluated pursuant to GISRA, including three systems that process classified information.

The audit took place from June through July 2002 and consisted of interviews, on-site observations, and reviews of Department and component documentation to assess WIN's and MNET's compliance with GISRA and related information security policies, procedures, standards, and guidelines.[1] We[2] used commercial-off-the-shelf and proprietary tools to conduct vulnerability tests and analysis of significant operating system integrity and security controls.

The interviews were conducted using the questionnaire contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, "Security Self-Assessment Guide for Information Technology Systems." This questionnaire contains specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be measured. The questionnaire contains 17 areas under 3 general controls (management, operational, and technical). The areas contain 36 critical elements and 225 supporting security control objectives and techniques (questions) about the system. The critical elements are derived primarily from the Office of Management and Budget (OMB) Circular A-130 and are integral to an effective information technology (IT) security program. The control objectives and techniques support the critical elements. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

The independent auditors assessed management, operational, and technical controls at a high risk to the protection of the WIN and MNET networks from unauthorized use, loss, or modification. Specifically, we identified vulnerabilities in 16 of the 17 control areas as indicated in the chart below:

[1] In a September 1997 audit, report number 97-26, the OIG recommended that the Department develop effective computer security program guidance. The Department then revised its policy and released DOJ Order 2640.2D in July 2001, which was used in the analysis of this year's review.

[2] In this report, "we" refers to either the OIG or to PwC working under the direction of the OIG.

CONTROL AREAS[3]	VULNERABILITIES NOTED
Management Controls	
1. Risk Management	
2. Review of Security Controls	√*
3. Life Cycle	√*
4. Authorize Processing (Certification and Accreditation)	√*
5. System Security Plan	√*
Operational Controls	
6. Personnel Security	√*
7. Physical and Environmental Protection	√*
8. Production, Input/Output Controls	√*
9. Contingency Planning	√*
10. Hardware and Systems Software Maintenance	√*
11. Data Integrity	√*
12. Documentation	√*
13. Security Awareness, Training, and Education	√*
14. Incident Response Capability	√*
Technical Controls	
15. Identification and Authentication	√*
16. Logical Access Controls	√*
17. Audit Trails	√*

Source: The OIG's FY 2002 GISRA audit of WIN and MNET.

√* Significant vulnerability in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur when a remote or local attacker violates the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

As a result of the findings identified in this report, we are providing recommendations for improving WIN and MNET systems to ensure that WIN and MNET management:

- Enforce the USMS policies and procedures developed to identify, track, correct, and maintain the corrected status of identified vulnerabilities.

- Ensure that a system development life cycle (SDLC) methodology is documented when planning, implementing, or maintaining a major application or general support system.

[3] Control Areas as described in the NIST SP 800-26 "Security Self-Assessment Guide for Information Technology Systems."

- Rescind the certification and accreditation and place WIN and MNET in an interim approval to operate (IATO) status pending the completion, at a minimum, of the security test & evaluation, contingency plan, and system security plan. Also, develop a corrective action plan establishing a schedule and milestones to complete the security test & evaluation, contingency plan and test, and system security plan while maintaining the IATO for no longer than six months.

- Modify WIN and MNET system security plans and USMS strategic plan to include the "Planning for Security in the Life Cycle" section, as described in NIST SP 800-18.

- Assign a group or person with the responsibility of addressing IT security and analyzing those controls that are deemed critical by USMS, to ensure MNET meets the requirements set forth in the upcoming/current C&A process. Maintain documentation evidencing the successful completion of each review and the corrective actions taken to address all issues identified. Finally, if the security controls surrounding MNET are not strengthened, MNET should be removed from production until all critical functions are properly secured.

- Establish procedures to ensure a separation of duties so that individuals responsible for developing the system are not tasked with either system or security administration.

- Implement Department's physical security controls as described in DOJ Order 2640.2D policy.

- Review all world-writeable files and directories. For any files and directories not needed for proper functioning of the system, the file permission should not be world-writeable. Users' files and directories permission settings should be set in a manner that is necessary for the user to fulfill job responsibilities and no more.

- Ensure that USMS management: (a) defines "umask" settings so that only the owner can view or modify files; (b) construct "path" variables so that no world-writeable directories are included in the path; and (c) ensure that all directories are searched appropriately in the "path" variable.

- Implement documented procedures for help desk personnel to follow when performing their daily responsibilities.

- Establish documented procedures to control how and when media and other types of USMS data are transferred.

- Complete a contingency plan for MNET and its associated applications and conduct a realistic test of the plan and adjust as indicated by the results of the test. Once the test results have been incorporated into the plan, obtain approval of the plan.

- Perform backups of the running configuration to the routers' onboard memory. All changes made to the configuration should be immediately backed up on a separate device. Where appropriate, use back up systems to ensure system availability. Cisco hardware offers advanced backup capabilities in case of hardware or software failure. Mission critical routers (typically core routers) may be good candidates to take advantage of Cisco backup capabilities.

- Remove software not required for business-related functions.

- Develop policies and procedures on the use of virus detection software and intrusion detection software and train individuals who will be monitoring the system.

- Create a system-warning banner. The warning message should be reviewed and approved by the USMS General Counsel.

- Develop policies and procedures for securing Cisco routers.

- Inquire with USMS General Counsel to determine which segments of the proposed *Rules of Behavior* document are delaying its approval, work with USMS General Counsel to establish a set of rules, and require all users to read and sign the *Rules of Behavior* document to ensure the users are aware of the contents.

- Define who in USMS is responsible for incident response.

- Enforce Department-wide identification and authentication policies to ensure that only authorized personnel can login to the system. Also, designate a system administrator to ensure accounts do not remain inactive on the system and ensure active accounts are appropriate.

- Enforce Department-wide password policies and procedures and install security tools on all servers to enforce restrictions on passwords.

- Remove accounts that do not require access to a privileged group.

- Develop, implement, and monitor policy establishing specific security standards and settings for running vulnerable services and server configurations.

- Require sensitive WIN data be encrypted before it is transferred across the network.

- Create an appropriate access list for all routers, and set timeout values for an unattended console.

- Activate Cisco routers' transmission control protocol (TCP) intercept mode and configure routers to allow logging of specific access lists.

- Implement and document policies and procedures requiring the latest security patches be obtained from the systems' vendor and that the patches are properly installed and configured.

- Develop, implement, and monitor documented policy for establishing specific password standards for Windows NT servers and ensure the policy is compliant with current Department policies.

- Implement procedures to ensure that system log messages are reviewed on a regular basis with system alerts being sent if problems arise.

Because of the significant vulnerabilities noted in this report, it is critical that the USMS take immediate corrective action on the above recommendations. We identified significant vulnerabilities in all but one control area. Specifically, we noted vulnerabilities in the following areas: review of security controls, life cycle, authorized processing, system security plan, personnel security, physical and environmental security, production and input/output controls, contingency planning, hardware and systems software maintenance, data integrity, documentation, security awareness, incident response capability, identification and authentication, logical access controls, and audit trails. We assessed these vulnerabilities as a high risk to the protection of WIN and MNET systems from unauthorized use, loss, or modification. If not corrected, certification and accreditation to operate the

WIN and MNET systems should be rescinded until all vulnerabilities are corrected.

We concluded that these vulnerabilities occurred because WIN and MNET management did not fully develop, enforce, or formalize agency-wide policies in accordance with current Department policies and procedures. Additionally, we believe the Department did not enforce its security policies and procedures to ensure that WIN and MNET systems were protected from unauthorized use, loss, or modification through the Department's certification and accreditation process. Furthermore, we believe many of the vulnerabilities identified during this audit could have been prevented if WIN and MNET management had followed-up on corrective actions for similar vulnerabilities identified in previous years.

TABLE OF CONTENTS

OBJECTIVE, SCOPE, AND METHODOLOGY

The fiscal year (FY) 2001 Defense Authorization Act (Public Law 106-398) includes Title X, subtitle G, "Government Information Security Reform Act" (GISRA). GISRA became effective on November 29, 2000, and amends the Paperwork Reduction Act of 1995 by enacting a new subchapter on "Information Security." It requires federal agencies to:

- Have an annual independent evaluation of their information security and practices performed.
- Ensure information security policies are founded on a continuous risk management cycle.
- Implement controls that appropriately assess information security risks.
- Promote continuing awareness of information security risks.
- Continually monitor and evaluate information security policies.
- Control effectiveness of information security practices.
- Provide a risk assessment and report on the security needs of the agencies' systems, and include the report in their budget request to the Office of Management and Budget (OMB).

The objective of the audit was to determine the U.S. Department of Justice's (Department) compliance with the requirements of GISRA. The United States Marshals Service's (USMS) Warrant Information Network (WIN) was selected as one of the subset of systems to be tested to determine the effectiveness of the Department's overall security program for FY 2002. WIN is accessed by both USMS district offices and headquarters users through the Marshal Network (MNET). Because of WIN's dependence on MNET, audit work was expanded to include MNET.

Under the direction of the Office of the Inspector General (OIG), and in accordance with Government Auditing Standards, PricewaterhouseCoopers LLP (PwC) performed the audit of WIN and MNET systems. In determining if the Department is compliant with GISRA requirements, PwC assessed whether adequate computer security controls existed to protect WIN and MNET systems from unauthorized use, loss, or modification.

The audit took place from June through July 2002. In this audit, we met with USMS officials from the Information Technology Services staff. We also met with representatives from the Department's Justice Management Division and the Chief Information Officer. We reviewed documentation that included the USMS's IT documents, organizational structures, OMB GISRA reporting information, and prior OIG reports to assess the WIN network's

compliance with GISRA and related information security policies, procedures, standards, and guidelines. We performed test work at the USMS headquarters in Arlington, Virginia.

The interviews were conducted using the questionnaire contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, "Security Self-Assessment Guide for Information Technology Systems." This questionnaire contains specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be measured. The questionnaire contains 17 areas under 3 general controls (management, operational, and technical). The areas contain 36 critical elements and 225 supporting security control objectives and techniques (questions) about the system. The critical elements are derived primarily from OMB Circular A-130 and are integral to an effective information technology (IT) security program. The control objectives and techniques support the critical elements. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

The audit approach was based on the General Accounting Office's Federal Information System Controls Audit Manual, the Chief Information Officer Council Framework, OMB Circular A-130, and guidance established by NIST. These authorities prescribe a review that evaluates the adequacy of management, operational, technical controls over control areas listed in Appendix I.

WIN AND MNET ENVIRONMENT

WIN contains the warrant, court records, internal correspondence related to the warrant, and other information on individuals for whom federal warrants have been issued. WIN is used to track the status of all federal warrants to aid in the investigations of all federal fugitives. It is also used to access the National Law Enforcement Telecommunication System (NLETS) and National Crime Information Center (NCIC) systems to obtain criminal record information from other federal, state, local and foreign law enforcement agencies participating in or cooperating with USMS fugitive investigations and apprehension efforts and to update the respective systems with new prisoner information.

WIN is accessed by both district offices and headquarters users through MNET, the backbone unclassified network for USMS operations. MNET is a sensitive but unclassified system that provides office automation tools to USMS personnel in carrying out their worldwide, mission-related

functions. MNET is accessible from field sites and from certain other federal agencies and commercial organizations.

SUMMARY RESULTS OF THE AUDIT

We tested to determine whether adequate computer security controls existed to protect WIN and MNET from unauthorized use, loss, or modification. Our testing consisted of assessing management, operational, and technical controls for 17 critical areas for WIN and MNET. Our testing disclosed vulnerabilities within 16 of the 17 areas. These vulnerabilities were identified as high risks to the protection of WIN and MNET. If not corrected, these security vulnerabilities threaten WIN's and MNET's data with the potential for unauthorized use, loss, or modification.

We concluded that these vulnerabilities occurred because WIN and MNET management did not fully develop, enforce, or formalize agency-wide policy in accordance with current Department policies and procedures. Additionally, we believe the Department did not enforce its security policies and procedures to ensure WIN and MNET were protected from unauthorized use, loss, or modification through its certification and accreditation process. Furthermore, we believe many of the vulnerabilities identified during this audit could have been prevented if USMS management had followed-up on corrective actions for similar vulnerabilities identified in previous years.

FINDINGS AND RECOMMENDATIONS

Our review disclosed that security controls need improvement to fully protect WIN and MNET from unauthorized use, loss, or modification. We found security vulnerabilities in all but one critical control area. Specifically, vulnerabilities were identified in the following areas: review of security controls; life cycle; authorize processing; system security plan; personnel security; physical and environmental protection; production and input/output controls; contingency planning; hardware and software maintenance; data integrity; documentation; security awareness, training and education; incident response capability; identification and authentication; logical access controls; and audit trails. The vulnerabilities identified in this report occurred because USMS management did not fully develop, enforce, or formalize agency-wide policy in accordance with current Department policies and procedures. Additionally, the Department did not enforce its security policies and procedures to ensure that WIN and MNET had been fully secured through its certification and accreditation process.

I. Management controls. Management controls are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

Management Controls	Vulnerabilities Noted
Risk Management	
Review of Security Controls	√*
Life Cycle	√*
Authorize Processing (Certification and Accreditation)	√*
System Security Plan	√*

√* Significant vulnerability in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur when a remote or local attacker violates the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

As a result of testing management controls, we confirmed that controls were adequate for WIN and MNET risk management. However, significant vulnerabilities were identified within the following management control areas:

A. Review of Security Controls. Routine evaluations and corrective actions on previously identified vulnerabilities are important elements of managing system risk. When significant weaknesses are identified, the

related risks should be reassessed, appropriate corrective actions taken, and follow-up monitoring performed to assure that corrective actions are effective.

Issue: Inappropriate Security Controls

Condition:

Independent reviews are only conducted once every three years. USMS does not conduct independent reviews when significant system changes or upgrades are implemented and completed. Additionally, weaknesses identified in prior reports, such as: "Independent Auditor's Report on Internal Control, Security Test & Evaluation Report," and "PricewaterhouseCoopers Penetration Testing Report" were still present at the time of our audit.

Cause:

USMS has ineffective procedures for identifying, tracking, and correcting weaknesses. Additionally, we found that USMS has an inadequate number of trained IT security personnel on its team to identify and correct weaknesses in a timely manner.

Criteria:

DOJ Order 2640.2D Chapter 1 Section 11(b), *Configuration Management*, states: "Components shall…Document and test all changes before modifying the accredited system and/or application so that new vulnerabilities are not introduced into the operational environment."

DOJ Order 2640.2D Chapter 1 Part 2, Section 7(e), *Certification and Accreditation*, states:

"The DAA shall:

- Evaluate the certification findings and assess vulnerabilities and residual risks.

- Approve corrective action and ensure its implementation."

Risk:

Without prompt management action to identify and correct weaknesses, WIN and MNET systems remain vulnerable.

Recommendation:

1. We recommend that the Director, USMS:
    a. Conduct independent reviews when significant system changes or upgrades are implemented and completed.

    b. Enhance and enforce USMS policies and procedures for identifying, tracking, and correcting vulnerabilities. Additionally, maintain a status report on corrective actions performed.

    c. Increase the number of trained IT security personnel in order to identify and correct system weaknesses in a timely manner.

B. Life Cycle. Like other aspects of an IT system, security is best managed if planned for the entire IT system life cycle. There are many models for the IT system life cycle, but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. Assessing a system's life cycle involves determining whether the following critical items are established: a system development life cycle methodology and system change controls that track a program's progress through testing to final approval.

Issue: Inadequate Systems Development

Condition:

The USMS currently does not have a documented and approved system development life cycle (SDLC) for WIN and MNET systems.

Cause:

USMS management is not committed to providing adequate resources to establish a formal documented methodology that describes how USMS personnel should develop, implement, and maintain systems.

Criteria:

DOJ Order 2640.2D Chapter 1, Part 6, *Information Technology Security Life Cycle,* states: "Components shall develop and implement a risk-based security process to provide security throughout the life cycle of all systems supporting their operations and assets."

Risk:

The absence of a documented and approved SDLC can lead to numerous complications in the development process that can cause system failures, system vulnerabilities and increases in project cost. In addition, inadequate software testing and planning can allow the system to enter production with major system flaws while also causing the project to go over budget.

Recommendation:

2. We recommend that the Director, USMS, ensure that a documented and approved SDLC methodology is applied when planning, implementing, or maintaining a major applications or general support systems.

C. Authorize Processing (Certification and Accreditation). Authorize processing provides a form of assurance of the security of the system. Computer security assurance is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. Certification is a formal process for testing components or systems against a specified set of security requirements while accreditation is a management official's formal acceptance of the adequacy of a system's security. Computer security accreditation forces managers and technical staff to work together to find workable, cost-effective solutions given security needs, technical constraints, operational constraints, and mission or business requirements.

Issue: Inadequate Documentation to Support Certification and Accreditation

Condition:

Several significant documents that support the certification and accreditation (C&A) of WIN and MNET systems are not complete. These documents include the systems' contingency plan, security test and evaluation (ST&E), and security plan. Therefore, the C&A requirements are not adequately fulfilled.

Cause:

According to USMS, there is an inadequate level of USMS resources (e.g., financial, human) to create these documents. As a result, the USMS individuals responsible for system accreditation are willing to accept high levels of risk.

Criteria:

DOJ Order 2640.D Chapter 1 Section 7, Certification and Accreditation, "Components shall ensure the certification and accreditation of all systems under their operational control.

a. All systems shall be certified and accredited prior to being placed into operation. Therefore, until an IT system is certified and accredited, no operational data can be used for any purpose, including testing in pilot systems if live data is used or if the pilot system is connected to a department network.

b. Each component shall designate a Certification Official for each system.

c. For each classified and sensitive but unclassified (SBU) system the Certification Official shall:

    (1) Ensure a system security plan is prepared and maintained throughout the system life cycle.
    (2) Ensure a risk analysis is performed to identify security risks, determine their magnitude, and identify areas needing safeguards.
    (3) Ensure a system test and evaluation is conducted and the results of such tests are documented.
    (4) Ensure Rules of Behavior and security procedures/guides are developed.
    (5) Ensure a contingency plan is prepared and tested.
    (6) Prepare the summary of compliance with the security requirements and the statement of residual risk.
    (7) Prepare a security evaluation report on the status of the certification and recommend to the Designated Approving Authority (DAA) whether or not to accredit the system based on documented residual risks.

(8) Prepare the accreditation grant for the DAA's signature.
(9) Submit the certification and accreditation package for classified systems to the Security and Emergency Planning Staff, JMD, and for SBU systems to the Information Management and Security Office (IMSO), JMD, for independent verification and validation."

Risk:

Allowing the system to be certified and accredited without adequate documentation of the risks of the system, system contingency plan, and security controls and with vulnerabilities present within the system increases the likelihood that the true security state of the system will be misconstrued and misrepresented.

Recommendation:

3. We recommend that the Director, USMS:

   a. Rescind the C&A and place WIN and MNET systems in an IATO status for no longer than six months while completing, at a minimum, the systems' ST&E, contingency plan, and security plan.

   b. Develop a corrective action plan establishing a schedule and milestones to complete the ST&E, contingency plan (including test of the contingency plan), and security plan within the six-month IATO period.

D. System Security Plans. A system security plan provides an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system.

Issue: Inadequate System Security Plan

Condition:

We found the security plan for WIN and MNET systems to be inadequate. The previously approved security plan for MNET does not include the security plan for WIN. Additionally, the MNET security plan is outdated because the system's interim authority has expired and the security plan

no longer meets the requirements set forth in that authority. Furthermore, USMS has no current strategic plan or similar document that discusses security plans at the component level.

Cause:

We found that USMS management is not committed to providing adequate resources to establish a formal security position that focuses on USMS security and is accountable for security plans. Additionally, the USMS security team has an inadequate number of trained security personnel to address corrective actions in a timely manner.

Criteria:

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, requires that all security plans for major systems or general support systems contain a section describing "Planning for Security in the Life Cycle."

Further, the system is governed by a condition in the MNET Accreditation Statement that states: "Based on my authority and judgment, and weighing the residual risks against operational requirements, I [the Designated Approving Authority (USMS's CIO)] authorize the interim operation of the USMS MNET Headquarters for six months to provide an opportunity for satisfactory resolution of the issues delineated in the SSAA [System Security Authorization Agreement] Appendix H. When these issues have been satisfactorily resolved, the USMS MNET Headquarters will be granted a full accreditation."

Risk:

Failing to mitigate risks identified during a C&A process that resulted in "an interim approval to operate," could potentially require the system to be taken out of production.

Recommendation:

4. We recommend that the Director, USMS, ensure that USMS management:

    a. Modify the WIN system security plan, USMS strategic plan, to include the "Planning for Security in the Life Cycle" section, as described in NIST SP 800-18.

b. Assign a group (or person) with the responsibility for correcting security vulnerabilities and analyzing those controls that are deemed critical by USMS to ensure WIN and MNET systems meet the requirements set forth in the upcoming/current C&A process and documenting all actions taken. Finally, if the security controls surrounding WIN and MNET are not strengthened, remove WIN and MNET from production until all critical functions are adequately secured.

II. Operational Controls. Operational controls address security controls that are implemented and executed by people. These controls are put in place to improve the security of a particular system. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

Operational Controls	Vulnerabilities Noted
Personnel Security	√*
Physical and Environmental Protection	√*
Production, Input/Output Controls	√*
Contingency Planning	√*
Hardware and Systems Software Maintenance	√*
Data Integrity	√*
Documentation	√*
Security Awareness, Training, and Education	√*
Incident Response Capability	√*

√* Significant vulnerability in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur when a remote or local attacker violates the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

Our testing identified vulnerabilities within all nine critical areas of operational controls. The specific details of the identified vulnerabilities are listed below.

A. Personnel Security. Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs.

Issue: Inadequate Separation of Duties

Condition:

WIN system security administration responsibilities are not adequately separated to ensure least privilege and individual accountability. The same individual is responsible for WIN application development, system administration, and system security.

Cause:

According to the USMS, there is an inadequate number of trained IT security personnel on the USMS security team to assume IT security administration responsibilities.

Criteria:

DOJ Order 2640.2D Chapter 2, Section 18 (l)(a) and (c), states: "Department IT systems shall have assignment and segregation of system responsibilities defined and documented…At a minimum, there shall be a clearly defined role for a security administrator and a system administrator." Additionally, "Controls [compliant with Department access control policies] shall be in place to ensure that the user [and administrators] has access to only the resources required to accomplish their duties and no more."

Risk:

Assigning the same individual to be responsible for development, system administration, and security administration grants a single individual the ability to change critical resources without authorization or detection. Additionally, this condition could potentially allow practices inconsistent with management intentions, requirements, acceptable security standards, and for segregation of duties to be compromised; thus, creating unnecessary risk.

Recommendation:

5. We recommend that the Director, USMS, establish procedures to ensure a separation of duties between individuals responsible for developing the system and those responsible for system or security administration.

B. Physical and Environmental Protection. Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment.

Issue: Inadequate Physical and Environmental Controls

Condition:

We found that physical and environmental controls surrounding the USMS computer room and building are inadequate. Backup tape rotation procedures, emergency exit and re-entry procedures, and fire and flood related controls are also inadequate. In addition, visitor access is not documented.

Cause:

This occurred because USMS management was not enforcing proper physical security.

Criteria:

DOJ Order 2640.2D, states: "Department IT systems shall be physically protected commensurate with the highest classification or sensitivity of the information. Department IT systems shall be environmentally protected, and the means for providing this protection shall be documented. Facilities supporting large scale IT operations, such as enterprise servers and telecommunication facilities, require consideration of additional environmental and physical controls as determined by a risk analysis."

Risk:

Insufficient physical and environmental controls can lead directly to major security incidents, such as theft and/or destruction, or to damage from accidental, natural or terrorist causes.

Recommendation:

6. We recommend that the Director, USMS, implement Department's physical security controls as described in DOJ Order 2640.2D.

Issue: World-Writeable Files

Condition:

We found two UNIX servers had 45,136 world-writeable files and directories including two files that are critical to system operation. Files and directories that are world-writeable allow any user on the system the ability to modify or delete their contents.

Cause:

Many of the world-writeable files and directories appeared to exist due to improper configuration of WIN on the part of USMS management.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states: "Enable the use of resources such as data and programs necessary to fulfill job responsibilities and no more."

Risk:

Improper configuration of home files directories could potentially allow a user to obtain the level of access of another identity on the server. If the compromise is business-critical, then this vulnerability is high-risk and could be exploited to gain privileged access on the server.

Recommendation:

7. We recommend that the Director, USMS, ensure that USMS management review all world-writeable files and directories. For any files and directories not needed for proper functioning of the system, the file permission should not be world-writeable. Users' files and directories permission settings should be set in a manner that is necessary for the user to fulfill job responsibilities and no more.

Issue: User Parameter Settings

Condition:

We found 16 files on 2 UNIX servers that contained improperly set "umask" values and 27 files on 2 UNIX servers that had insecure "path" variables. The "umask" variable is used for default file-creation permissions. Unsafe "umask" settings allow users, other than the owner of the file, read and or write permissions to files. This increases the risk that unauthorized users view, delete, or modify sensitive or proprietary information.

Cause:

These conditions appear to exist due to the USMS's improper configuration of the "path" variables and "umask" values.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16 (a) and (f), *Access Control,* states that the system must: "Enable the use of resources such as data and programs necessary to fulfill job responsibilities and no more …Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Insecure PATH variables increase the risk that users will be deceived by common system commands such as list files, which are executed instead of the system list files. For example, an unauthorized user could write a program that performs certain functions and call the program list files. When an authorized user invokes the list files command, the bogus list files program would be executed.

Recommendation:

8. We recommend that the Director, USMS, ensure that USMS management:

    a. Define the "umask" settings so that only the owner can view or modify files.

b. Construct "path" variables so that no world-writeable directories are included in the path.

c. Ensure that all directories are searched appropriately in the "path" variable.

C. Production and Input/Output Controls. There are many aspects to IT operations support. Topics range from a user help desk to procedures for storing, handling, and destroying media.

Issue: Help Desk Policies and Procedures Do Not Exist

Condition:

A system help desk is designed to offer advice and respond to system security incidents in a timely manner, and assist users with the operation of the system and applications (including the re-setting of user passwords). At the time of our audit, USMS did not implement adequate security controls pertaining to its help desk operation. Specifically, we noted that USMS do not have documented procedures for help desk personnel to follow when assisting WIN and MNET users. Additionally, no controls exist to ensure that users' account passwords are properly reset when accounts are locked, or when users forget their passwords.

Cause:

According to USMS personnel, the shortage of personnel on the USMS IT security team has resulted in an inability to handle the associated responsibilities and daily tasks required to maintain a secure computing environment and help desk operations that are compliant with Department policy.

Criteria:

NIST SP 800.18, Section 5.MA.3, states: "...provide a synopsis of the procedures in place that support the operations of the application such as using questions like, 'Is there a help desk or group that offers advice and can respond to security incidents in a timely manner? Are there procedures in place documenting how to recognize, handle, and report incidents and/or problems...'"

Risk:

Without documented help desk policies and procedures, unauthorized individuals could potentially exploit the help desk by fraudulently presenting themselves as an authorized user, which could allow them to change passwords and obtain unauthorized access. Unauthorized individuals could potentially gain access to sensitive USMS data, allowing them to make personal gains based on the type of data.

Recommendation:

9. We recommend that the Director, USMS, ensure that USMS management implement documented procedures for help desk personnel to follow when performing their daily responsibilities.

Issue: Media Controls

Condition:

No documented process has been established to ensure only authorized individuals can pick up, receive, or deliver input/output information and media. In addition, no formal process has been established to ensure adequate audit trails are maintained for inventory management of such media.

Cause:

According to USMS personnel there are inadequate numbers of trained security personnel on the USMS security team to handle the associated responsibilities.

Criteria:

USMS Manual Section 9.2-2, *Limited Official Use Information*, states: "Limited Official Use (LOU) information used by USMS must be maintained, distributed, secured and disposed of in a manner that will protect the information against unauthorized disclosure. This section sets forth the requirements for safeguarding unclassified but sensitive information."

DOJ Order 2640.2D Section 19, *Accountability and Audit Trails*, states: "…Maintain an audit trail of activity sufficient to reconstruct security relevant events."

Risk:

Without documented procedures for media security controls, unauthorized individuals could potentially obtain access to sensitive USMS data. This condition could potentially allow practices inconsistent with management intentions, requirements, and acceptable security standards.

Recommendation:

10. We recommend that the Director, USMS, establish documented procedures to control how and when media and other types of USMS data are transferred. An audit trail should also be maintained to evidence such events.

D. Contingency Planning. Contingency planning ensures continued operations by minimizing the risk of events that could disrupt normal operations and having an approach in place to respond to those events should they occur.

Issue: No Documented Contingency Plan Exists

Condition:

Contingency plans were not documented or tested for the MNET and WIN systems.

Cause:

According to USMS, there is a shortage of trained security personnel on the USMS security team resulting in the inability to develop a contingency plan.

Criteria:

Section 9.4-10 Contingency Planning, of the USMS Manual states, "Contingency planning is required to ensure continuity of ADP operations to the greatest degree possible of data processed or stored by the ADP

systems. Contingency plans will be generated for each ADP facility and will be submitted to the Computer Systems Program Manager for review and approval upon generation. Approved contingency plans will be tested by personnel from each ADP facility at least once annually to ensure adequacy of scope and operation. Any deficiencies noted by the test will result in a revision to the contingency plan and resubmission to the Computer Systems Program Manager."

Risk:

Without a comprehensive, tested contingency plan, USMS management cannot be assured of the ability to restore critical systems in a timely fashion following a disaster or significant service interruption.

Recommendation:

11. We recommend that the Director, USMS, ensure that USMS management complete a contingency plan for MNET and its associated applications and conduct a realistic test of the plan and adjust as indicated by the results of the test. Once the test results have been incorporated into the plan, obtain approval of the plan.

Issue: Cisco Router Fault Tolerance is Inadequate

Condition:

We found fault tolerance controls are inadequate on the Cisco router. Backup configuration files are stored inadequately and the Cisco router does not take advantage of backup capabilities.

Cause:

According to USMS personnel, these conditions are due to lack of additional hardware for fault tolerance purposes.

Criteria:

DOJ Order 2640.2D Chapter 2, Security Program Management Contingency Planning/Business Resumption Planning, states: "Components shall plan for how they will perform their missions in the event their IT systems are unavailable and how they will recover these IT systems in the event of loss or failure."

Risk:

If the running configuration becomes corrupt, the router will boot with the startup configuration stored in its memory. It is essential that configuration is kept up-to-date.

Recommendation:

12. We recommend that the Director, USMS, ensure that USMS management performs backups of the running configuration to the routers' onboard memory. All changes made to the configuration should be immediately backed up on a separate device. Where appropriate, use backup systems to ensure system availability. Cisco hardware offers advanced backup capabilities in case of hardware or software failure. Mission critical routers (typically core routers) may be good candidates to take advantage of the Cisco backup capabilities.

E. Hardware & Software Maintenance. These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes.

Issue: System Software

Condition:

The winsvr server contains a compiler, which does not support a business need.

Cause:

This condition appears to exist due to USMS not knowing the software was on the system.

Criteria:

USMS Security Policy and Procedures Manual - Volume IX Section 9.4-19, System Software, states: "Software which is not used for official USMS operations shall not be loaded onto USMS ADP systems and any such software already present on ADP systems upon receipt from a vendor or manufacturer shall be purged from the system upon receipt."

Risk:

Inappropriate use of software on the server might lead to potential risks including, but no limited to, service disruption and legal issues.

Recommendation:

13. We recommend that the Director, USMS, ensure that USMS management remove any software not required for business-related functions.

F. Data integrity. Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and integrity.

Issue: Inadequate Data Integrity, Validation Controls, and Virus Detection Controls

Condition:

Although virus detection software is installed on MNET workstations, virus detection and elimination software are not installed on the application servers. Additionally, workstation virus detection software is not updated in a timely manner.

Cause:

A shortage of trained security personnel on the USMS security team resulted in the USMS not being able to install and update virus detection software for all of its systems.

Criteria:

DOJ Order 2640.2D, Chapter 3 Section 35, states: "All Department IT systems shall employ virus protection software. Anti-virus software shall:

- Detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways.

- Be enabled on workstations and servers at start-up and employ resident scanning.

- On servers, update virus signature files immediately, or as soon as possible, with each new release."

Risk:

The lack of virus detection software leaves the system vulnerable to common types of virus and possibly corruption or disruption of system services.

Recommendation:

14. We recommend that the Director, USMS, ensure that USMS management develops policies and procedures to ensure the installation and use of virus detection software and intrusion detection software and train individuals to use it properly.

Issue: Warning Banner

Condition:

The *winsrv* server does not display a system-warning banner when users log onto the server.

Cause:

We concluded that USMS personnel were not aware that there was a requirement for a system-warning banner.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 18, *Password Management*, states: "All Department IT systems shall implement a system banner that provides warnings: to employees that accessing the system constitutes consent to system monitoring for law enforcement and other purposes; and to unauthorized users that their use of the system may subject them to criminal prosecution and/or criminal or civil penalties."

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Section 3.3.1, states: "The many different components of risk should be examined. This examination normally includes gathering data about the threatened area and synthesizing and analyzing the information to make it useful. The types of areas are...Vulnerability Analysis. A vulnerability is a condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat."

Risk:

The *winsrv* server provides information to users before they are authenticated to the server. It is important to inform users of the sensitive nature of the resources they are using. In attempting to gain useful information for compromising the server, an unauthorized user could use this information. The USMS's ability to prosecute criminals may be undercut by its inability to prove they abused systems knowing they were to be used only for official purposes. It is also a good practice to proactively inform users they are subject to audit.

Recommendation:

15. We recommend that the Director, USMS, ensure that USMS management creates a system-warning banner. The warning message should be reviewed and approved by the USMS's General Counsel.

G. Documentation. Documentation refers to the descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and that formalize the system's security controls. Assessing documentation involves evaluating the USMS's efforts to complete the following critical requirements:

- There is sufficient documentation that explains how software/hardware is to be used.
- There are documented formal security and operational procedures.

Issue: Cisco Router Policies

Condition:

We found no documented policies for securing existing Cisco routers and implementing future routers.

Cause:

We concluded that USMS management has not placed a high priority on documenting router policies.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states: "Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

Proper security policies and operating procedures for routers and supporting devices are essential for maintaining the networking environment

Recommendation:

16. We recommend that the Director, USMS, ensure that USMS develop, as well as implement, policies and procedures for securing Cisco routers.

H. Security Awareness, Training, and Education. People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge.

Issue: No "Rules of Behavior" Document Has Been Approved

Condition:

No Rules of Behavior document has been approved by USMS to provide guidance on how to use USMS systems. In addition, users have not been given adequate training and education regarding rules of behavior.

Cause:

USMS developed a *Rules of Behavior* document that contains relevant information for users to follow while using USMS systems. However, USMS requires the General Counsel approval before distribution to users. Unfortunately, the General Counsel has failed to return or validate the proposed *Rules of Behavior* in a timely manner, preventing the distribution of this document.

Criteria:

DOJ Order 2640.2D, Chapter 1 Section 7, states: "For each classified and SBU system the Certification Official shall...Ensure Rules of Behavior and security procedures/guides are developed."

Risk:

The lack of a *Rules of Behavior* document could potentially have several negative effects. For example, users could choose an action that violates the Department's requirements inadvertently or out of ignorance. Also, USMS could potentially be unable to hold certain users accountable for their actions given the lack of express instructions describing appropriate activities.

Recommendation:

17. We recommend that the Director, USMS, ensure USMS management:

    a. Inquire with the General Counsel to determine which segments of the proposed *Rules of Behavior* document are delaying the approval and work with the General Counsel to establish a set of rules that meets Department's requirements.

b. Require all users, including both government and contract employees, to read and sign the *Rules of Behavior* document to ensure the users are aware of the contents.

I. Incident Response Capability. Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact can be far-reaching.

Issue: Formal Incident Response Procedures Have Not Been Established

Condition:

We found that USMS has no written incident response procedures.

Cause:

According to USMS personnel, there is a shortage of trained IT security personnel on the USMS security team, preventing USMS from establishing written incident response policies and procedures.

Criteria:

DOJ Order 2640.2D, Chapter 1 Section 5, states: "For SBU systems, security incidents that meet the criteria established by the Department of Justice Computer Emergency Response Team (DOJCERT) shall be reported by the component to DOJCERT within time frames established by DOJCERT."

Risk:

Without a clear definition of responsibilities for incident response, the likelihood that an incident will not be handled properly and in accordance with USMS and Department procedures is increased, which could increase the harm to the system or decrease the effectiveness of a response.

Recommendation:

18. We recommend that the Director, USMS, ensure that USMS management define responsibilities for incident response, and

coordinate and complete an agreement that clearly states who is responsible for incident response for USMS.

III. TECHNICAL CONTROLS. Technical controls focus on security controls that the computer system executes and depend upon the proper functioning of the system to be effective. Technical controls also require significant operational considerations and should be consistent with the management of security within the organization.

We assessed the effectiveness of operational and technical controls on WIN and MNET systems by using commercial off-the-shelf and proprietary software to conduct penetration testing on the system. A penetration test is a security test in which evaluators attempt to access sensitive information on the system to determine whether appropriate security controls are in place.

Technical Controls	Vulnerabilities Noted
Identification and Authentication	√*
Logical Access Controls	√*
Audit Trails	√*

√* Significant vulnerability in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur when a remote or local attacker violates the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

As a result of testing USMS technical controls, we confirmed that controls were not adequate.

A. Identification and Authentication. Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users.

Issue: User Account Management Is Improperly Configured

Condition:

- Two out of 144 accounts on *winsrv* do not have a valid business need.

- Duplicate root-equivalent accounts (both have a user identification (UID) of 0) exist on hq001.

- Users are not required to log in as unprivileged users from any terminal, except the console, on winsrv and hq001.

- Users who must access a shared account, such as root, are not required to first log in with an individual account and then be switched to the shared account on winsrv and hq001.

- No formal process has been established by USMS to describe authorized users and their associated access privileges.

Cause:

- The accounts that do not have a valid business need appear to be unnecessary default accounts that were never removed.

- The duplicate root-equivalent accounts appear to exist only for the matter of convenience.

- Users are not required to log in as unprivileged users from other servers because of the convenience.

- Users who must access a shared account (such as root) are not being required to first log in with an individual account and then be switched to root because of the convenience.

- No formal process has been established by USMS to describe authorized users and their associated access privileges because USMS currently does not assign the responsibility of security (and/or user management) to a specific individual who has the resources and experience to properly secure this environment.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states that the system must: "Enable the use of resources such as data and programs necessary to fulfill job responsibilities and no more."

DOJ Order 2640.2D, *Identification And Authentication,* states: "No later than February, 2003, secure privileged accounts by using authentication technology stronger than that which is based only on a UserID and password."

USMS Security Policy and Procedures Manual - Volume IX Section 9, *ADP System User Access Authentication*, states: "Each user will have a unique user identification and password."

Risk:

Providing access on the server to users without a business need significantly increases security risks. Additionally, duplicate user identifications increase the risk that unauthorized users will modify or delete files created by another user, and jeopardize accountability. Furthermore, duplicate root-equivalent accounts increase the risk that users have system access privileges that are not required for their job functions. Furthermore, unauthorized users who target root-equivalent accounts have multiple opportunities to gain root access.

Allowing users to log into the system directly as root from any host on the network increases the risk that an unauthorized user will gain privileged access to the system. If shared accounts are logged into directly, then accountability is lost. Allowing inactive accounts to remain on the system could potentially give unauthorized users a vehicle or target for gaining unauthorized access to sensitive system resources.

Recommendation:

19. We recommend that the Director, USMS, ensure that USMS management:

    a. Enforce Department-wide identification and authentication policies and ensure that only authorized personnel can login to the system.

    b. Establish a system administrator to ensure accounts do not remain inactive on the system and ensure active accounts are appropriate.

Issue: Password Controls are inadequate

Condition:

In the USMS's "PwC Penetration Testing Vulnerability Report," dated June 19, 2000, it was disclosed that USMS's UNIX and Novell servers had weak passwords (UNIX Finding 1, UNIX Finding 5 and Novell Finding 1).

At the time of our audit, we identified the following related weaknesses:

- USMS Security Policy and Procedures Manual - Volume IX Section 9, ADP System User Access Authentication, states: "Passwords shall be six alphanumeric characters in length…," which is in violation of current Department policy.

- Four out of 172 accounts on two UNIX servers had passwords equal to the users' names.

- Ninety-nine out of 154 accounts on one UNIX server had the same password.

- One UNIX server had the maximum password age set at 99,999 days.

- One UNIX server had two files that contain passwords in clear text.

- Thirty-nine accounts on five Novell servers have a null password.

Cause:

- USMS passwords policy conflicts with Department policy because USMS has not reviewed and updated the policy to ensure compliance with the Department's requirement.

- Accounts with passwords that are equal to the users' name exist because initial default passwords have not been changed.

- The 99 accounts that have the same passwords are used by WIN administrators and have been assigned the same password as a matter of convenience.

- The password age set at 99,999 days is due to a misconfiguration of the UNIX server on the behalf of USMS.

- The two files with passwords in clear text are used for automatic login for such services as file transfer protocols.

- The cause of all of the Novell accounts with null passwords appears to be an oversight on the behalf of USMS.

Criteria:

DOJ Order 2640.2D, Chapter 2 Section 18(b)(1), *Password Management*, states: "Department IT systems that use passwords as the means for authentication shall implement…An eight-character password composed of at least three of the following: English uppercase, English lower case, numerics, special characters."

USMS Security Policy and Procedures Manual - Volume IX
Section 9, *ADP System User Access Authentication,* states: "... each user will have a unique user identification and password."
DOJ Order 2640.2D, Chapter 2 Section 18(b)(3) and (4), *Password Management,* states: "Limit password lifetime to a maximum of 90 days," and "Prevent the display of a clear text password."

Risk:

Inconsistent policies can lead to security weaknesses. In this case, the USMS policy permits weaker passwords than the Department's policy allows.

Easy-to-guess passwords increase the chances that an intruder can gain access to the system or represent him or herself as a valid user. This was proven by our ability to gain root access on one UNIX server using the default password of a UNIX account. Furthermore, having the same password for multiple accounts increases the chance that users can log in with a different account and thus masquerade their identity.

Account passwords that are not changed with a scheduled frequency increase the possibility of compromise and unauthorized use of the account by an intruder representing him or herself as a valid user.

The existence of reference files or scripts with unencrypted passwords increases the risk that unauthorized users will gain access to user accounts on the system.

Users without passwords increase the risk that unauthorized users will gain access to systems and access data and system configuration files.

Recommendation:

20. We recommend that the Director, USMS:

    a. Review and update its current policies so that they are in compliance with the Department's policies.

    b. Enforce Department-wide password policies and procedures and install security tools on all servers to enforce restrictions on passwords.

Issue: Accounts and Privileged Groups

Condition:

On the *hq001* server, 2 out of 177 accounts are inappropriately assigned to privileged groups. Users listed in privileged groups have access to group files and directories owned by the privileged group. This increases the risk that sensitive system configuration files could be changed or deleted.

Cause:

This condition exists due to a misconfiguration on the part of USMS.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control,* states: "Enable the use of resources such as data and programs necessary to fulfill job responsibilities and no more."

Risk:

Users listed in privileged groups have access to group files and directories owned by the privileged group. This increases the risk that sensitive system configuration files could be changed or deleted.

Recommendation:

21. We recommend that the Director, USMS, ensure that USMS management delete accounts that do not require access to a privileged group.

B. Logical Access Controls. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

Issue: Logical Access Controls

Condition:

The following risky services are found to be running on WIN and MNET systems:

- "rusers" (found on one server) – "rusers" provides information about users on the host.
- Telnet (found on 16 servers) – allows userid and password information to pass over the network as clear text.
- Berkley r-services (rexec, rlogin, rsh) and configuration files (/etc/hosts.equiv) (found on 14 servers) – allow users to log in or execute commands from a trusted machine without re-authenticating.
- .rhosts (found on two servers) – individual .rhost files (in conjunction with r-services), allow users to log in or execute commands from a trusted machine with out re-authenticating.
- Sendmail (vrfy and expn commands)(found on six servers) – provides email transport.

The following Windows NT server configurations were set improperly in all Windows NT Primary Domain Controllers (PDC) servers accessed:

- Five allow "anonymous" connections to gather user, group, share, and policy information.
- Five had no account lockout, including the administrator account.
- Five did not have the auditing feature enabled. Auditing is critical for preventing and monitoring unauthorized access to the Windows NT environment.

- Seven servers has "finger daemon," which gives out information including username, login status, and last login time.

Similar conditions relating to rusers, telnet, Berkley r-services, vrfy and expn, finger, and other services were also noted in the following prior-year findings (USMS PwC Penetration Testing Vulnerability Report, dated June 2000, Finding numbers: 2, 4, 6, 7, 10, 12, 14, and 15.)

Cause:

- Rusers are enabled by default.
- Telnet offers a major convenience for users.
- The Berkley r-services offer a convenience to users.
- The vrfy and expn sendmail commands are enabled by default.
- The finger command is enabled by default.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states: "Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

- Rusers (found on one server) – Rusers provides potentially enticing information on users on the host. It provides information on how busy the machine is and on login accounts. This is information an intruder can use in an attack. A scanner or attacker in a brute-force attack can then use the account information.
- Telnet (found on 16 servers) – allows userid and password information to pass over the network in the clear. Any unauthorized user on the network can sniff out this information and log into the system as that user.
- Berkley r-services (rexec, rlogin, rsh) (found on 14 servers) and configuration files (/etc/hosts.equiv and rhosts – found on two servers). r-services (rexec, rlogin and rsh) (in conjunction with the /etc/hosts.equiv file) and individual .rhosts files, provide a large

amount of risk to a system by allowing users to log in or execute commands from a trusted machine without re-authenticating;

- Sendmail (vrfy and expn commands)(found on six servers) – provides email transport. There are features and bugs to sendmail that may place the system at risk and could allow unauthorized access or remote execution of programs.

- Five servers allow "anonymous" connections to gather user, group, share, and policy information. Anonymous connections give individuals a method of obtaining share, group, user, and account policy and account lockout information from a system.

- Five servers had no account lockout, including the administrator account. Locking out accounts after a specified failed login attempts decreases the risk that the user accounts will be compromised through brute force attacks.

- Five servers did not have the auditing feature enabled. Auditing is critical for preventing and monitoring unauthorized access to the Windows NT environment.

- Seven servers had finger daemon, which gives out information including username, login status, last login time, and other information that an unauthorized user could use to plan an attack on the system.

Recommendation:

22. We recommend that the Director, USMS, ensure that USMS management develop, implement, and monitor procedures establishing specific security standards and settings for running vulnerable services and server configurations.

Issue: Data Encryption

Condition:

Encryption is not being used to protect WIN data that is sent across MNET.

Cause:

USMS does not require WIN data to be encrypted before transmission.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states: "Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Federal Information Processing Standards Publication (FIPS PUB) 46-3, states: "Data that is considered sensitive by the responsible authority, data that has a high value, or data that represents high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage."

Risk:

Sensitive information may be the target of sniffing attacks by unauthorized users. If transactions are occurring that contain highly confidential information, it may be vulnerable to sniffing if it is not encrypted. Hash algorithms will help mitigate against a loss of data integrity should the data be manipulated in transit.

Recommendation:

23. We recommend that the Director, USMS, implement some level of encryption of WIN data before it is transferred across the network.

Issue: Cisco Router Access Controls Are Inadequate

Condition:

The following router access controls are inadequate on the Cisco router:

- Access lists are not used to restrict which hosts can access the login prompt.

- The router does not have a session-timeout variable assigned. Timeout sessions provide additional security against consoles that are left unattended.

Cause:

We found that these conditions exist due to misconfiguration of the setting by USMS.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states: "Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure," and "Disable inactive sessions so that authentication is required to re-establish the session after 20 minutes or less of inactivity. Screen saver or workstation lockouts that require users to re-enter their passwords, such as those available in Windows, are acceptable."

DOJ Order 2640.2D Chapter 2 Section 18, *Password Management*, states: "All Department IT systems shall implement a system banner that provides warnings: to employees that accessing the system constitutes consent to system monitoring for law enforcement and other purposes; and to unauthorized users that their use of the system may subject them to criminal prosecution and/or criminal or civil penalties."

Risk:

Allowing anyone on the network access to the login prompt increases the risk of unauthorized access to the router.

Timeout sessions provide additional security against consoles that are left unattended. If a user can gain access to a console left unattended, they can modify the router's configuration.

Recommendation:

24. We recommend that the Director, USMS, ensure that USMS management create an appropriate access list for all routers, and set timeout values for an unattended console.

Issue: Cisco Router Traffic Filtering

Condition:

Traffic filtering controls are inadequate on the Cisco router. The router does not have transmission control protocol (TCP) intercept mode activated, which is used to watch the activity of incoming connection requests to aid in the prevention of a denial of service attack. Additionally, activity not explicitly allowed is not being logged to an access list. The information obtained from the access list can be used to examine unwarranted attempts to access the network.

Cause:

These conditions exist because of USMS's misconfiguration of the TCP intercept mode.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states: "Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

USMS Security Policy and Procedures Manual - Volume IX Section 9, *ADP System User Access Authentication*, states: "Audit trails are required on all ADP systems processing Limited Official Use or classified information which may be accessed by more than one user and must be reviewed by the Computer Systems Security Officer or Assistant Computer Systems Security Officer at least on a weekly basis."

Risk:

If TCP intercept mode is not activated, WIN becomes susceptible to denial of service attacks, which can shut down the network.

If access lists are not used to monitor activity, unauthorized users may be able to gain access to the router.

Recommendation

25. We recommend that the Director, USMS, ensure that USMS security management properly configure TCP intercept mode and add logging for specific access lists.

Issue: Software Patches

Condition:

We found that the operating system software is not kept up-to-date with respect to security patches on the *winsrv* and *hq001* servers. Current versions of the software patch contain processing and security enhancements. Additionally, the patch can correct bugs that have been identified by (or communicated to) the operating system vendor.

Cause:

This condition exists due to a lack of formal procedures for keeping up-to-date with security patches.

Criteria:

NIST SP 800-13 Section 5.10, *Telecommunications Security Guidelines for Telecommunications Management Network,* states*:* "All new software features and patches shall be tested first on a development system and approved by an appropriate testing organization, prior to installation on an operational system. Tests that modify live data shall not be performed. A risk analysis shall be conducted of proposed software changes to determine their impact on network element security. Any changes to security features or security defaults shall be documented and made available to the user before the software is distributed."

Risk:

If the version of the operating system and the security patches are not current, there is an increased risk that an unauthorized user may be able to exploit system weaknesses.

Recommendation:

26. We recommend that the Director, USMS, ensure USMS management implement and document procedures to require that the latest security patch from the system vendor is obtained and that it is properly installed and configured.

Issue: Windows NT Systems Improperly Configured.

Condition:

Windows NT systems' configuration were improperly set, as identified below:

- The following Windows NT Primary Domain Controllers (PDCs) allow anonymous connections to gather user, group, share, and policy information:

  ABSSERVER
  HRD_PS7NT
  COLOSSUS
  JSD-APPS
  HQ_NOTES

- The following Windows NT PDCs have a minimum password length of 0 characters:

  ABSSERVER
  HRD_PS7NT
  COLOSSUS
  HQ_NOTES

- The following Windows NT PDCs have no maximum password age:

  HRD_PS7NT
  JSD_APPS

- The following Windows NT PDCs have the minimum password age set to 0 days:

  ABSSERVER
  HRD_PS7NT
  COLOSSUS
  JSD_APPS
  HQ_NOTES

- The following Windows NT PDCs have a password history of 0 passwords:

  ABSSERVER
  HRD_PS7NT
  COLOSSUS
  HQ_NOTES

Similar conditions were also noted in a prior year (June 2000) report, as identified below:

- The following prior-year findings relate to Windows NT PDCs allowing null connections to gather information:
  "Windows NT Finding 4" in the "USMS PwC Penetration Testing Vulnerability Report"

- The following prior-year findings relate to account lockout:
  "Windows NT Finding 6" in the "USMS PwC Penetration Testing Vulnerability Report"
  "Windows NT Finding 7" in the "USMS PwC Penetration Testing Vulnerability Report"

- The following prior-year finding relates to auditing not being enabled:
  "Windows NT Finding 8" in the "USMS PwC Penetration Testing Vulnerability Report"

Cause:

All of the conditions noted above exist due to a lack of formal Windows NT security procedures.

Criteria:

DOJ Order 2640.2D Chapter 2 Section 16, *Access Control*, states: "Protect the system, its data and applications, from unauthorized disclosure, modification, or erasure."

Risk:

- The null credentials logon gives individuals a method of obtaining share, user and group, account policy, and account lockout information from a system. With this information, attackers can start brute force guessing passwords and attempt to compromise the system.

- Setting a minimum password length forces users to create passwords that will be more difficult to guess or crack.

- Account passwords that are not periodically changed increases the possibility of compromise and exposure to the password. It also increases the possibility of unauthorized access to the system.

- By setting a minimum password age, users are prevented from cycling passwords until they return to their previous password. Having this feature enabled prevents a user from bypassing the password uniqueness control.

- Requiring unique passwords prevents a user from recycling old passwords that may have been compromised.

- Users in the "Domain Admins" group have the highest level of privileges on a Windows NT Domain, and are thus the first target of unauthorized users. The more "Domain Admins" there are, the more avenues of attack there are for an unauthorized user to gain access.

- Inactive accounts are often used by intruders to break into a network.

- Locking out accounts after a specified number of failed login attempts decrease the risk that user accounts will be compromised through brute force attacks.

- Auditing is crucial for preventing and monitoring unauthorized access to the Windows NT environment.

Recommendation:

27. We recommend that the Director, USMS, ensure that USMS management develop, implement, and monitor documented policy establishing specific password standards for server configurations.

C. Audit trails. Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems.

Issue: Auditing, Logging, and Monitoring Are Not Sufficient.

Condition:

System activities are not adequately logged and reviewed on a regular basis on *winsrv* and *hq001* servers.

Cause:

This condition exists due to a lack of formal procedures for auditing.

Criteria:

USMS Security Policy and Procedures Manual - Volume IX Section 9, *ADP System User Access Authentication*, states: "Audit trails are required on all ADP systems processing limited official use or classified information which may be accessed by more than one user and must be reviewed by the Computer Systems Security Officer or Assistant Computer Systems Security Officer at least on a weekly basis."

Risk:

Insufficient logging will result in the lack of an audit trail in the event of an unauthorized access. Without good logging and monitoring, administrators are not often given early warnings for hardware and software errors or problems.

Recommendation:

28. We recommend that the Director, USMS, ensure that USMS management implement procedures to ensure that system log messages are reviewed on a regular basis and that system alerts are sent when problems arise.

CONCLUSION

We assessed management, operational, and technical controls at a high risk to the protection of the WIN and MNET systems from unauthorized use, loss, or modification. Specifically, we identified vulnerabilities in 16 of the 17 control areas and noted security findings in the following areas: review of security controls, life cycle, authorized processing, system security plan, personnel security, physical and environmental security, production and input/output controls, contingency planning, hardware and systems software maintenance, data integrity, documentation, security awareness, incident response capability, identification and authentication, logical access controls, and audit trails. Certification and accreditation to operate the WIN and MNET systems should be rescinded until these weaknesses are corrected.

We concluded that these vulnerabilities occurred because USMS management did not fully develop, enforce, or formalize agency-wide policies in accordance with current Department policies and procedures. Additionally, the Department did not enforce its security policies and procedures to ensure the WIN and MNET systems were protected from unauthorized use, loss, or modification through its certification and accreditation process. Furthermore, many of the vulnerabilities identified during this audit could have been prevented if USMS security management had followed-up on corrective actions for similar vulnerabilities identified in previous years.

Additionally, many of the causes stated in this report evidence a lack of commitment by USMS to implement timely corrective actions. This is illustrated by the inadequate number of individuals on the IT security team assigned to develop the documents required for WIN and MNET certification and accreditation.

APPENDIX I

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GENERAL AREAS OF CONTROL

The review focused on evaluating the adequacy of management, operational and technical controls over the following specific control areas:

I. MANAGEMENT CONTROLS. Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

- **Risk Management.** Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Assessing risk management involves evaluating the USMS efforts to complete the following critical procedures:

    - Periodic performance of a system risk assessment had been performed.
    - Program officials understand the risk to systems under their control and had determined the acceptable level of risk.

- **Review of Security Controls.** Routine evaluations and response to identified vulnerabilities are important elements of managing security controls of a system. Determining whether review of security controls had been adequately performed requires the auditor to assess if the following critical items were completed:

    - A system security control review had been performed for both WIN and MNET and interconnected systems.
    - Management ensured effective implementation of corrective actions.

- **Life Cycle.** Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation,

operation, and disposal. Assessing a system's life cycle involves identifying if the following critical items are in place for WIN and MNET:

- A system development life cycle methodology.
- System change controls as programs progress through testing to final approval.

- **Authorize Processing (Certification and Accreditation).** Authorize processing (also referred to as certification and accreditation) provides a form of assurance of the security of the system. To determine whether WIN and MNET had been appropriately authorized to process data involves analyzing critical documents that identifies whether:

  - The system had been certified/recertified and authorized to process (accredited).
  - The system is operating on an interim authority in accordance with specified agency procedures.

- **System Security Plan.** A system security plan provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. Assessing whether the WIN and MNET systems have an adequate system security plan requires identifying if the following critical elements were met:

  - A system security plan had been documented for the system and all interconnected systems if the boundary controls are ineffective.
  - The plan is kept current.

II. OPERATIONAL CONTROLS: Operational controls address security controls that are implemented and executed by people. These controls are put in place to improve the security of a particular system. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

- **Personnel Security.** Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their

jobs. Assessing personnel security involves evaluating the USMS efforts to complete the following critical procedures:

  - Duties are separated to ensure least privilege and individual accountability.
  - Appropriate background screening for assigned positions is completed prior to granting access.

- **Physical and Environmental Protection.** Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing physical and environmental protection involves evaluating the USMS efforts to complete the following critical procedures:

  - Adequate physical security controls have been implemented and are commensurate with the risks of physical damage or access.
  - Data is protected from interception.
  - Mobile and portable systems are protected.

- **Production, Input/Output Controls**. There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling, and destroying media. Assessing production, input/output controls involves evaluating the USMS efforts to ensure the following critical elements are met:

  - User support is being provided to WIN and MNET network users.
  - Media controls are in place for the WIN and MNET network.

- **Contingency Planning.** Contingency planning ensures continued operations by minimizing the risk of events that could disrupt normal operations and having an approach in place to respond to those events should they occur. Assessing contingency planning involves evaluating the USMS efforts to complete the following critical procedures:

  - Identify the most critical and sensitive operations and their supporting computer resources.
  - Develop and document a comprehensive contingency plan.
  - Have tested contingency/disaster recovery plans in place.

- **Hardware and System Software Maintenance.** These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a

historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. Assessing hardware and system software maintenance involves evaluating the USMS efforts to complete the following critical procedures:

  - Access is limited to system software and hardware.
  - All new and revised hardware and software are authorized, tested, and approved before implementation.
  - Systems are managed to reduce vulnerabilities.

- **Data Integrity.** Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. Assessing data integrity involves evaluating the USMS efforts to complete the following critical procedures:

  - Virus detection and elimination software is installed and activated.
  - Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.

- **Documentation.** The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. Assessing documentation involves evaluating the USMS efforts to complete the following critical procedures:

  - There is sufficient documentation that explains how software/hardware is to be used.
  - There are documented formal security and operational procedures.

- **Security Awareness, Training, and Education.** People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. Assessing security awareness, training, and education involves evaluating the USMS efforts to complete the following critical procedures:

- Employees have received adequate training to fulfill their security responsibilities.

- **Incident Response Capability.** Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching. The following questions are organized according to two critical elements. Assessing incident response capability involves evaluating the USMS efforts to complete the following critical procedures:

  - There is a capability to provide help to users when a security incident occurs in the system.
  - Incident related information is shared with appropriate organizations.

III. TECHNICAL CONTROLS. Technical controls focus on security controls that the computer system executes and depend upon the proper functioning of the system to be effective. Technical controls require significant operational considerations and should be consistent with the management of security within the organization.

- **Identification and Authentication.** Identification and authentication is a technical measure that prevents unauthorized people or processes form entering an IT system. Access Control usually requires that the system be able to identify and differentiate among users. Authentication is verification that a person's claimed identity is valid and it is usually implemented through the use of passwords. Assessing identification and authentication involves evaluating the USMS efforts to complete the following critical procedures:

  - Users are individually authenticated via passwords, tokens, or other devices.
  - Access controls are enforcing segregation of duties.

- **Logical Access Controls.** Logical Access Controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Assessing logical Access Controls involves evaluating the USMS efforts to complete the following critical procedures:

- Logical access controls restrict users to authorized transactions and functions.
- There are controls over network access.
- There controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

- **Audit Trails.** Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. Assessing audit trails involves evaluating the USMS efforts to complete the following critical procedure:

    - Activity involving access to and modification of sensitive or critical files is logged, monitored, and possible security violations are investigated.

U.S. Department of Justice

United States Marshals Service

Office of the Director

October 29, 2002

MEMORANDUM TO: Glen A. Fine
Inspector General

ATTN: Guy K. Zimmerman
Assistant Inspector General for Audit

FROM: Benigno G. Reyna
Director

SUBJECT: Draft Audit Report – The United States Marshals Service's Warrant Information Network Independent Evaluation Pursuant to the Government Information Security Reform Act fiscal Year 2002

Attached is the U.S. Marshals Service response to the findings and recommendations contained in the referenced report. I appreciate the seriousness of the issues raised in the report and have directed appropriate staff to develop a plan of action to address them.

We are committed to developing an information technology system within the Department of Justice that meets established policies and regulations.

Attachment

Warrant Information Network (WIN) - Draft OIG Audit Report
October 2002

Management Controls

Issue	Recommendation	USMS Response
1. Inappropriate Security Controls	a. Conduct independent reviews when significant changes are implemented and completed. b. Enhance and enforce USMS policies and procedures for identifying, tracking, and correcting vulnerabilities. Maintain a status report on corrective actions performed. c. Increase the number of trained IT security personnel in order to identify and correct system weaknesses in a timely manner.	The USMS currently conducts reviews of systems and applications on an ongoing basis in support of DOJ C&A requirements. This ongoing review process, as well as other independent reviews and audits, identified many of the same or related findings as included in the OIG WIN audit. The USMS developed a corrective action plan to track and resolve IT security vulnerabilities identified in previous years' financial audits. Periodic status reports (weekly and monthly) were provided to the UKW auditors as part of the FY 2001 financial audit. While some progress has been made, resolution of many of the system vulnerabilities requires additional security resources. The USMS has repeatedly sought more security funding and personnel, but to date, support for these requests has not been forthcoming from the Department.
2. Inadequate Systems Development	Ensure that a documented and approved System Development Life Cycle (SDLC) methodology is applied when planning, implementing, or maintaining major applications or general support systems.	The USMS has developed an Information Technology Investment Management (ITIM)/SDLC process. The USMS ITIM/ SDLC process was approved by the DOJ CIO in August 2002. The process will be implemented in USMS in FY 2003.

3. Inadequate Documentation to Support Certification and Accreditation (C&A)	a. Rescind the C&A and place WIN and MNET systems in an Interim Approval To Operate (IATO) status for no longer than 6 months while completing, at a minimum, the systems' system test & evaluation plan (ST&E), contingency plan, and security plan. b. Develop a corrective action plan establishing a schedule and milestones to complete the ST&E, contingency plan (including test of the contingency plan), and security plan within the 6 months IATO period.	The USMS concurs with placing WIN and MNET in an IATO status for 6 months while completing the recertification and reaccreditation process for the systems. A corrective action plan will be established to complete the required C&A documents within the 6 month timeframe, including preparing the ST&E, contingency plan (with testing), and system security plan.
4. Inadequate System Security Plan	a. Modify the WIN system security plan, USMS strategic plan, to include the "Planning for Security in the Life Cycle" section, as described in NIST SP 800-18. b. Assign a group (or person) with the responsibility for correcting security vulnerabilities and analyzing those controls that are deemed critical by USMS to ensure WIN and MNET systems meet the requirements set forth in the upcoming/current C&A process and documenting all action taken. Finally, if the security controls are not strengthened, remove WIN and MNET from production until all critical functions are adequately secured.	As part of the recertification and reaccreditation for WIN and MNET, the system security plan and required SDLC documents will be prepared or modified to comply with NIST requirements. ITS personnel will be assigned to implement necessary security controls. Corrective actions will be taken so that WIN and MNET are adequately secured as it is not feasible to take these systems out of production.

Operational Controls

Issue	Recommendation	USMS Response
5. Inadequate Separation of Duties	Establish procedures to ensure a separation of duties between individuals responsible for developing the system and those responsible for system or security administration.	The USMS has procedures in place requiring separation of duties between system developers and system administrators. However, IT staffing limitations have precluded the procedures from being effectively enforced. Support from the Department for USMS IT security budget requests would rectify this problem.

6. Inadequate Physical and Environmental Controls	Implement Department's physical security controls as described in DOJ Order 2640.2D.	Enhancements were recently made to the USMS HQ Penthouse to improve physical and environmental controls for IT systems. All USMS production servers have been moved to the Penthouse, and further physical and environmental controls will be implemented as funding permits.
7. World-Writeable Files	Review all world-writeable files and directories. For any files and directories not needed for proper functioning of the system, the file permission should not be world-writeable. Users' files and directories permission settings should be set in a manner that is necessary for the user to fulfill job responsibilities no more.	The USMS will review the status of all WIN files and directories on the WIN servers and will develop procedures for proper assignment of file permissions for users. A policy of "least privilege" system access will be implemented.
8. User Parameter Settings	a. Define the "umask" settings so that only the owner can view or modify files. b. Construct "path" variables so that no world-writeable directories are included in the path. c. Ensure that all directories are searched appropriately in the "path" variable.	The USMS will review the status of all WIN files and directories on the WIN servers and will develop procedures for proper assignment of user parameters.
9. Help Desk Policies and Procedures Do Not Exist	Implement documented procedures for help desk personnel to follow when performing their daily responsibilities.	The USMS agrees that written procedures need to be prepared to assist help desk personnel in responding to user problems. It should be noted, however, that help desk personnel are not responsible for resolving security problems (e.g., resetting user passwords). Rather, security issues are referred by help desk personnel to system administrators or security staff for resolution. Deployment of the Justice Consolidated Office Network (JCON) in USMS will facilitate help desk support and significantly improve security through implementation of a standard PC and server set-up and institution of rigorous configuration control.

10. Media Controls	Establish documented procedures to control how and when media and other types of USMS data are transferred. An audit trail should also be maintained to evidence such events.	Written media control procedures and audit trails will be established to protect and monitor access to sensitive USMS data.
11. No Documented Contingency Plan Exists	Complete a contingency plan for MNET and its associated applications and conduct a realistic test of the plan and adjust as indicated by the results of the test. Once the test results have been incorporated into the plan, obtain approval of the plan.	The USMS is in the process of preparing a contingency plan for MNET as part of the recertification and reaccreditation process. The plan will be tested and revisions made as appropriate.
12. Cisco Router Fault Tolerance is Inadequate	Perform backups of the running configuration to the routers' onboard memory. All changes made to the configuration should be immediately backed up on a separate device. Where appropriate, use backup systems to ensure system availability. Cisco hardware offers advanced backup capabilities in case of hardware or software failure. Mission critical routers (typically core routers) may be good candidates to take advantage of the Cisco backup capabilities.	The USMS will institute policy and procedures to ensure all stable running router configuration files are archived. Additionally, the USMS is reviewing its current inventory of routers and service plans to ensure adequate fault tolerance/recovery is in place. Finally, the USMS will be implementing Cisco Works for router configuration management.
13. System Software	Remove any software not required for business-related functions.	The USMS concurs and will do this as part of the JCON deployment. JCON will preclude loading of software on PCs for non-business-related functions.
14. Inadequate Data Integrity, Validation Controls, and Virus Detection Controls	Develop policies and procedures to ensure the installation and use of virus detection software and intrusion detection software and train individuals to use it properly.	It should be noted that virus detection software is loaded on every Windows-based computer. Additionally, virus protection policies and procedures will be developed for use by trained IT personnel. The JCON platform will provide for automatic update of virus definition files.
15. Warning Banner	Create a system-warning banner. The warning message should be reviewed and approved by the USMS's General Counsel.	A system warning banner has already been established for WIN as well as for USMS financial systems and the authentication server. OGC will be consulted as to any necessary changes to the existing language. Warning banners will be implemented on all all USMS systems as appropriate.

16. Cisco Router Policies	Develop, as well as implement, policies and procedures for securing Cisco routers.	The USMS concurs with developing and implementing policies and procedures for securing Cisco routers.
17. No "Rules of Behavior" Document Has Been Approved	Inquire with the General Counsel to determine which segments of the proposed *Rules of Behavior* document are delaying the approval and work with the General Counsel to establish a set of rules that meets the Department's requirements.	ITS will work with General Counsel to finalize Rules of Behavior to comply with Department guidance.
18. Formal Incident Response Procedures Have Not Been Established	Define responsibilities for incident response, and coordinate and finalize an agreement that clearly states who is responsible for incident response for USMS.	A Computer Incident Response Plan was prepared in October 2002. The plan includes designation of incident response responsibilities.

Technical Controls

Issue	Recommendation	USMS Response
19. User Account Management Is Improperly Configured	a. Enforce Department-wide identification and authentication policies and ensure that only authorized personnel can login to the system. b. Establish a system administrator to ensure accounts do not remain inactive on the system and ensure active accounts are appropriate.	The USMS concurs with enforcing Departmental identification and authentication polices, allowing only authorized personnel to login to the system, and ensuring proper activation of user accounts.
20. Password Controls Are Inadequate	a. Review and update current policies so that they are in compliance with the Department's policies. b. Enforce Department-wide password policies and procedures and install security tools on all servers to enforce restrictions on passwords.	The USMS will ensure its policies conform to DOJ guidance and will enforce them. Security tools will be installed on servers to enforce password restrictions.
21. Accounts and Privileged Groups	Delete accounts that do not require access to a privileged group.	The USMS will delete accounts that do not require access to a privileged group.
22. Logical Access Controls	Develop, implement, and monitor procedures establishing specific security standards and settings for running vulnerable services and server configurations.	The USMS will establish specific security standards and settings for running vulnerable services and server configuration through development, implementation, and monitoring of procedures.

23. Data Encryption	Implement some level of encryption of WIN data before it is transferred across the network.	The USMS will review what level of WIN data encryption is necessary and implement accordingly.
24. Cisco Router Access Controls are Inadequate	Create an appropriate access list for all routers, and set timeout values for an unattended console.	The USMS will review our policies regarding access lists for routers and revise as appropriate. A 20 minute timeout will be set.
25. Cisco Router Traffic Filtering	Ensure that USMS security management properly configure TCP intercept mode and add logging for specific access lists.	The USMS will review its router configurations and adjust as appropriate, based on the policies and procedures developed in response to item #16.
26. Software Patches	Implement and document procedures to require that the latest security patch from the system vendor is obtained and that it is properly installed and configured.	Procedures will be developed and implemented to ensure software patches are obtained from system vendors in a timely manner and tested prior to installation.
27. Windows NT Systems Improperly Configured	Develop, implement, and monitor document policy establishing specific password standards for server configurations.	The USMS will establish, disseminate, and enforce password policies and standards.
28. Auditing, Logging, and Monitoring Are Not Sufficient	Implement procedures to ensure that system log messages are reviewed on a regular basis and that system alerts are sent when problems arise.	Respon sibility will be assigned to USMS personnel to review system logs on a regular basis and transmit system alerts regarding identified problems.

OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

Recommendation Number:

1. **Resolved.** The USMS agreed with the need for appropriate security controls and stated that while some progress has been made, resolution of many of the system vulnerabilities requires additional security resources. To close this recommendation, the USMS needs to provide the OIG evidence of the USMS's corrective action plan to track and resolve IT security vulnerabilities.

2. **Resolved.** The USMS agreed with the need to implement a System Development Life Cycle (SDLC). To close this recommendation, the USMS needs to provide the OIG with evidence that the Information Technology Investment Management/SDLC methodology was approved and implemented.

3. **Resolved.** The USMS agreed to place WIN and MNET in an Interim Approval To Operate (IATO) status for six months. To close this recommendation, the USMS needs to provide the OIG evidence that an IATO is obtained and a corrective action plan is established within the six month timeframe, including preparing the ST&E, contingency plan (with testing), and a system security plan.

4. **Resolved.** The USMS agreed with the need for an adequate WIN system security plan. To close this recommendation, the USMS needs to provide the OIG with evidence that the system security complies with NIST requirements and that corrective actions were taken to ensure WIN and MNET systems meet the requirements set forth in the C&A process.

5. **Resolved.** The USMS agreed with the need for proper separation of duties and stated that procedures are in place requiring separation of duties. To close this recommendation, the USMS needs to provide the OIG with the procedures requiring separation of duties between system developers and system administrators.

6. **Resolved.** The USMS agreed with the need for adequate physical and environmental controls and indicated all USMS production servers had been moved to a new location. To close this recommendation, the USMS needs to provide the OIG evidence that the new location's

physical and environmental controls were implemented as described in DOJ Order 2640.2D.

7. **Resolved.** The USMS agreed with the need to review world-writeable files. To close this recommendation, the USMS needs to provide the OIG evidence that the (a) WIN files and directories were reviewed, (b) procedures were developed for proper assignment of file permissions for users, and (c) the policy of "least privilege" was implemented.

8. **Resolved.** The USMS agreed with the need to review the use of parameter settings. To close this recommendation, the USMS needs to provide the OIG evidence that the user parameter settings were reviewed for proper assignment of user parameters.

9. **Resolved.** The USMS agreed that written procedures need to be prepared to assist help desk personnel in performing their daily responsibilities. To close this recommendation, the USMS needs to provide the OIG evidence that written procedures are in place to assist help desk personnel in responding to user problems.

10. **Resolved.** The USMS agreed that written media control procedures and audit trails need to be established. To close this recommendation, the USMS needs to provide the OIG evidence once documented procedures are established to control how and when media and other types of USMS data are transferred. In addition, please provide documentation showing how audit trails will be maintained to evidence such events.

11. **Resolved.** The USMS agreed that a documented MNET contingency plan is needed. To close this recommendation, the USMS needs to provide the OIG evidence that a contingency plan is approved and tested.

12. **Resolved.** The USMS agreed that Cisco router fault tolerance is inadequate. To close this recommendation, the USMS needs to provide the OIG evidence that policies and procedures are implemented to ensure all stable runner router configuration files are archived.

13. **Resolved.** The USMS agreed with the need to remove system software that is not required. To close this recommendation, the USMS needs to provide the OIG evidence once the Justice Consolidated Office Network (JCON) deployment has been performed

showing the removal of any software not required for business-related functions.

14. **Resolved.** The USMS agreed with the need to develop policies and procedures for virus and intrusion detection. To close this recommendation, the USMS needs to provide the OIG the policies and procedures developed to ensure the installation and use of virus detection software and intrusion detection software. In addition, please provide evidence that IT personnel are receiving training to use the software properly.

15. **Resolved.** The USMS agreed with the need to create a system-warning banner. To close this recommendation, the USMS needs to provide the OIG evidence showing creation of a system-warning banner that was reviewed and approved by the USMS's Office of General Counsel (OGC).

16. **Resolved.** The USMS agreed with the need to develop and implement policies and procedures for securing Cisco routers. To close this recommendation, the USMS needs to provide the OIG evidence that policies and procedures are developed and implemented.

17. **Resolved.** The USMS agreed with the need to establish *Rules of Behavior*. To close this recommendation, the USMS needs to provide the OIG evidence that the OGC was contacted and the *Rules of Behavior* finalized to comply with Department guidance.

18. **Resolved.** The USMS stated in their response that a Computer Incident Response Plan, including designation of incident response responsibilities, was prepared in October 2002. To close this recommendation, the USMS needs to provide the OIG with a copy of the Computer Incident Response Plan.

19. **Resolved.** The USMS concurred with enforcing Department-wide identification and authentication policies. To close this recommendation, the USMS needs to provide the OIG evidence that a process is established to enforce the Department-wide policies and a system administrator is established to ensure accounts do not remain inactive on the system and active accounts are appropriate.

20. **Resolved.** The USMS concurred that password controls are inadequate. To close this recommendation, the USMS needs to provide the OIG evidence that the password policies were updated in

compliance with Department's policies. In addition, please provide the OIG evidence that security tools are installed on servers to enforce password restrictions.

21. **Resolved.** The USMS agreed to delete accounts that do not require access to a privileged group. To close this recommendation, the USMS needs to provide the OIG evidence that the accounts were deleted.

22. **Resolved.** The USMS agreed to establish security standards and settings for running vulnerable services and server configuration. To close this recommendation, the USMS needs to provide the OIG with the security standards and settings that are established.

23. **Resolved.** The USMS agreed to review the level of WIN data encryption. To close this recommendation, the USMS needs to provide the OIG evidence of the level of encryption implemented before data is transferred across the network.

24. **Resolved.** The USMS agreed to review Cisco router access controls. To close this recommendation, the USMS needs to provide the OIG with the an updated access list for all routers and documentation showing that a 20 minute timeout is set for an unattended console.

25. **Resolved.** The USMS agreed to review and incorporate changes to its router configurations. To close this recommendation, the USMS needs to provide the OIG with evidence that procedures include properly configuring TCP intercept mode and logging for specific access lists.

26. **Resolved.** The USMS agreed to develop and implement procedures for security patches. To close this recommendation, the USMS needs to provide the OIG evidence that the security patch is obtained from the vendor in a timely manner and tested prior to installation.

27. **Resolved.** The USMS agreed to establish, disseminate, and enforce password policies and standards. To close this recommendation, the USMS needs to provide the OIG evidence that the USMS developed, disseminated, and monitors its password policies and standards.

28. **Resolved.** The USMS agreed to assign a person to review system logs on a regular basis and transmit system alert when problems arise. To close this recommendation, the USMS needs to provide the OIG with the USMS personnel assigned responsibility for reviewing system logs. In addition, the USMS needs to provide the OIG with the procedures

implemented to ensure that system logs messages are reviewed on a regular basis and that system alerts are sent when problems arise.